UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,340	10/25/2001	Gavin A. McLintock	34118	4956

116 7590 03/21/2005

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
TRUONG, LAN DAI T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/004,340	MCLINTOCK ET AL.	
	Examiner	Art Unit	
	lan dai thi truong	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *03/12/05, 05/03/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: Reply to Status Inquiry

DETAILED ACTION

Claim rejections-35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

1) Claims 1-5, 8, 10, 13, 15-18, 20, 24-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Martin et al. (U.S 5,979,754), herein after referred to as Martin

In referring to claim 1, the limitations:

1a) "A communications network" is matched (Martin: abstract, lines 1-17; column 3, lines 62-67; column 4, lines 9-22)

Martin discloses a door control apparatus useable in buildings or other facilities having many locked doors or rooms and requiring controlled access to the room. Martin discloses a method of using paging transmitters and paging receivers to transmit information from a central control system to individual door control units located at each controlled door. Martin's door control system meets the limitation "A communications network."

1b)"A door/key administering system for storing a key unique to each of the users, for storing an identification code unique to each of the doors, and for assigning access authorization to at least one user for each door, the door/key administering system being communicatively connected to the communications network" is matched (Martin: column 3, lines 42-57; column 4, lines 66-67; column 5, lines 1-32)

Martin discloses a door control apparatus utilized a "control system includes a computer for store and process data" which is equivalent to "door/key administering system" may be located at a central control center that includes a computer programmed to store the identity of all doors and rooms requiring the control in a given facility. The program will also include an identification of all individuals authorized to have entry to all or specific room of the facility and can associate a specific entry card with each room and each authorized person. Martin discloses control system assigns a guest an available room, stores the credit card identity information and informs the guest that the credit card is a key for the assigned room. Martin discloses that the computer will be operatively associated with paging transmitter to broadcast instructions directed to particular door locks to program each of the door locks to allow a predetermined entry card or cards to open those locks. Martin's door control system is shared identical functionality with the limitation "A door/key administering system for storing a key unique to each of the users, for storing an identification code unique to each of the doors, and for assigning access authorization to at least one user for each door, the door/key administering system being communicatively connected to the communications network."

1c) "A door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in

response to the authorization for access, The door lock/control assembly being communicatively connected to the door/key administering system via the communications network" is matched (Martin: column 6, lines 6-67; column 4, lines 4-45; column 3, lines 47-55; column 4, lines 9-22; column 5, lines 1-32)

Martin discloses "entry card reader" which is equivalent to "door lock/control" is positioned adjacent each guest room door. Martin discloses that when the guest runs the proper "credit card" which is equivalent to "room key" through his/her guest room card reader, a door lock release apparatus at the guest room door will open the lock, this process is shared identical functionality with the limitation "A door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in response to the authorization for access." Furthermore, Martin discloses a method of using paging transmitters and paging receivers to transmit information from a central control system to individual door control units located at each controlled door. If the "computer" which is equivalent to "door/key administering system" recognizes and accepts that guest card as an approved key, then computer generates a signal which is sent to the door transceiver causing the lock to open to an "approved card" which is equivalent to " room key." Martin's door control system meets the limitation "The door lock/control assembly being communicatively connected to the door/key administering system via the communications network."

1d) "Whereby a user can gain access to the doors authorized to the user with a unique key" is matched (Martin: column 3, lines 47-55, column 4, lines 15-16)

Martin discloses "guest's credit card" is equal to "unique key" for the assigned room. When the guest runs the proper credit card through his/her guest room card reader, a door lock

release apparatus at the guest room door will open the lock. Martin's door control system meets the limitation "Whereby a user can gain access to the doors authorized to the user with a unique Key."

In referring to claims 2 and 3 the limitation:

1e) "Wherein the access given to a particular key to a particular door is communicated to the door/key administrator by the door control/lock assembly; wherein the door control/lock assembly reads the key presented by a user and sends the read to the door/key administering system to obtain access authorization" is matched (Martin: abstract, lines 6-12; column 3, lines 47-57; column 5, lines 1-32; column 4, lines 21-45, 62-67)

Martin discloses the "guest's credit card" is "a particular key" for the assigned room. When the guest runs the "proper credit card" is "room key" through his/her "guest room card reader" what is equivalent to "the door control/lock assembly", if the "computer" which is equivalent to "door/key administrator" recognizes and accepts that the "guest card" as an "approved key" which is equivalent to "room key", the computer generates a signal that is sent to door transceiver causing the lock to open to an "approved card." Martin's door control system meets the limitation "Wherein the access given to a particular key to a particular door is communicated to the door/key administrator by the door control/lock assembly; wherein the door control/lock assembly reads the key presented by a user and sends the read to the door/key administering system to obtain access authorization."

In referring to claim 4, the limitation:

1f) "Wherein the door control/lock assembly carries out the authorization process when the communication between the door assembly and the door/key administering system is interrupted" is matched (Martin: column 4, lines 21-45, 62-67; column 7, lines 30-44)

Martin discloses that after the guest runs the "proper credit card" is "room key" through "his/her guest room card reader" which is equal to "the door control/lock assembly", the "computer" which is equal to "door/key administering system" recognizes and accepts that the guest card as an approved key, then a signal is transmitted to the door transceiver causing the lock to open to an approved card, so this process is shared identical functionality with the limitation "Wherein the door control/lock assembly carries out the authorization process when the communication between the door assembly and the door/key administering system is interrupted."

In referring to claims 5and 24, the limitation:

1g) "Wherein the communications network includes wireless communications network" is matched (Martin: abstract: lines 1-17; column 3, lines 62-67; column 4, lines 9-22, 58-62)

Martin discloses a door control apparatus useable in buildings or other facilities having many locked doors or rooms and requiring controlled access to the room. Martin discloses the method of using wireless communication to transfer information between the "computer" which is equivalent to "door/key administering system" located lock control center and guest room card reader located at guest room. Martin's door control system meets the limitation "Wherein the communications network includes s wireless communications network."

In referring to claims 8, 16, the limitation:

1h) "Wherein the key includes a key signature unique to the respective user and recognizable by the door control/lock assembly, the key signature being a numeric code, a sequence of numbers, a unique signal, or a biometric recognition code" is matched (Martin: column 3, lines 44-56; column 4, lines 15-16)

Martin discloses that "the credit card is a key for the assigned room" which is equal to "the key signature being a numeric code, or sequence number". Martin discloses when the guest runs the proper credit card through his guest "room card reader" which is equal to "door control/lock assembly", then door lock release apparatus at the guest room door will open the lock, this process is shared functionality with the limitation "the key includes a key signature unique to the respective user and recognizable by the door control/lock assembly". Martin's door control system meets the limitation "Wherein the key includes a key signature unique to the respective user and recognizable by the door control/lock assembly, the key signature being a numeric code, a sequence of numbers, a unique signal, or a biometric recognition code."

In referring to claim 10, the limitation:

1i) "An identification device for reading the key presented by the users" is matched (Martin: column 3, lines 44-56)

Martin discloses a guest room "credit card reader" which is equal to "an identification device" for reading the "credit card" which is equivalent to "room key" presented by the users. Martin's door control system meets the limitation "An identification device for reading the key presented by the users."

1j"A lock adapted to be operated in response to the authorization from the door/key administering system; an embedded controller for controlling the operation of the identification

device and the lock, and the authorization process" is matched (Martin: column 4, lines 1-45, 65-67; column 5, lines 1-30)

Martin discloses if the "computer" which is equivalent to "door/key administering system" that is located at a central control center recognizes and accepts that guest card as an approved card, then the computer generates a signal which is sent to door transceiver causing the lock to open to an "approved card" which is equivalent to "room key". Martin's door control system meets the limitation "A lock adapted to be operated in response to the authorization from the door/key administering system; an embedded controller for controlling the operation of the identification device and the lock, and the authorization process."

In referring to claim 13, the limitation:

1k) "Wherein the door assembly is connected wirelessly to the communications network, and the door control/lock assembly further includes a wireless transmitter/receiver" is matched Martin: column 4, lines 1-67; column 5, lines 1-30)

Martin discloses method of using wireless communication to transfer information between the "computer" which is equivalent to "door/key administrator" that is connected to transmitter and "the guest room card reader" which are equivalent to "the door control/lock assembly" that is connected to guest room door wireless receiver so as to actuate the door lock release apparatus. Martin disclosed method of using wireless communication between transmitter and guest room door wireless receivers. Martin's method meets the limitation "Wherein the door assembly is connected wirelessly to the communications network, and the door control/lock assembly further includes a wireless transmitter/receiver."

In referring to claim 15, the limitation:

11) "Wherein the embedded controller includes a database for storing information on the keys and users such that, when the communication between the door assembly and the door/key administering system is interrupted. The door control/lock assembly can carry out the authorization process for the door associated therewith" is matched (Martin: abstract, lines 6-12; column 3, lines 42-57; column 5, lines 1-32; column 4, lines 21-45, 62-67; column 7, lines 30-44)

Martin discloses "computer" which is equivalent to "database" for storing information on "the guest's credit cards" which is equivalent to "room keys", identity of all doors and rooms requiring control in given facility, and identification of all individuals authorized to have entry to all or specific rooms of facility and can associate a "specific card" which is equal to "room key" with each room and each authorized person. Martin also discloses when the guest runs the proper credit card through his/her guest room card reader, if the computer which be located at central control center recognizes and accepts that "guest card" as an "approved key" then computer generates a signal which is sent to the door transceiver causing the lock to open to an "approved card" which is equivalent to "room key." Martin's door control system meets the limitation "Wherein the embedded controller includes a database for storing information on the keys and users such that, when the communication between the door assembly and the door/key administering system is interrupted. The door control/lock assembly can carry out the authorization process for the door associated therewith."

In referring to claim 17, the limitation:

1m) "Wherein the key/door administering system is physically separated into a key administering system and a door administering system" is matched (Martin: abstract, lines 1-17; column 19-10, lines column 4, lines 66-67; column 5, lines 1-46)

Martin discloses the door control system relates to the field of "guest registration system" which is equivalent to "key administering system" is located at a central control center, and "door control unit" which is equivalent to "door administering system" is located at guest room. The guest registration system and door control unit cooperate to cause the lock to open to an "approved card" which is equivalent to "room key." Martin's door control system meets limitation "Wherein the key/door administering system is physically separated into a key administering system and a door administering system."

In referring to claim 18, the limitation:

1n) "Wherein the stored data pertaining to the keys and the doors can be updated when required" is matched (Martin: column 3, lines 42-49; column 4, lines 66-67; column 5, lines 1-11; column 7, lines 30-44)

Martin discloses a "control system" which is equivalent to "the guest registration system" includes a computer programmed to include the identity of all doors, rooms and a list of "specific entry card" is equivalent to "room key" with each room and each authorized person. Martin discloses the guest registration system will assign the guest an available room, and "store" is equal to "update" the credit card identity information as a key for assigned room. Then upon check-out from the place of lodging, the computer simply "removes" is equal to "updates" the credit card identity information from the memory and cared ceases to function as a guest room key, this process is shared functionality with the limitation "the stored data pertaining to

the keys and the doors can be updated when required." Martin's door control system meets the limitation "Wherein the stored data pertaining to the keys and the doors can be updated when required."

In referring to claim 20, the limitation:

1o) "Storing a unique identification code for each of the doors in a server; storing a unique key signature for each of the users in the server; assigning to each door the unique Keys having access authorization to the respective doors; comparing a user's key detected at the door to the keys having access authorization to the door in the server; authorizing access to the door; wherein the authorization step is carried out through the communications network between the door and the server and each user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or user assigned thereto" is matched (Martin: column 3, lines 42-57; column 4,lines 22-45; column 5, lines 1-30; column 7, lines 30-44)

Martin discloses "the computer" which is equivalent to "server" stores the identity of all doors and rooms requiring control in a given facility, and identification of all individuals authorized to have entry to all or specific rooms of the facility and can associate a "specific entry card" which is equivalent to "room key" with each room and each authorized person, that meets the limitation "Storing a unique identification code for each of the doors in a server; storing a unique key signature for each of the users in the server; assigning to each door the unique Keys having access authorization to the respective doors." Also, Martin discloses if the computer recognizes and accepts the guest card as an approved key after the guest runs the proper credit card through his guest room card reader, the computer then generates a signal that is sent to room

transceiver causing the lock to open to an "approved card" which is equivalent to " room key," that meets the limitation "wherein the authorization step is carried out through the communications network between the door and the server and each user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or user assigned thereto."

In referring to claim 25, the limitation:

1p) "The systems being communicatively and operatively connected to a communication network. A Meta server being adapted to server as an address reference among the door access control and key management systems, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each door access control and key management system and its associated unique key ID codes and unique door ID codes and each door access control and key management system contains the address of the Meta Server" is matched (Martin: column 3, lines 42-57, lines 62-67; column 4, lines 1-45; column 5, lines 1-32)

Martin discloses a "the computer" which is equivalent to "Meta server" which stores the identity of all doors and rooms requiring control in a given facility, and identification of all individuals authorized to have entry to all or specific rooms of the facility and can associate a specific entry card with each room and each authorized person. Also Martin discloses a method of using paging transmitters and paging receivers to transmit information from "computer" as "Meta server" at central control system to individual door control units located at each controlled door. Martin's door control system meets the limitation "The systems being communicatively

and operatively connected to a communication network; a Meta server being adapted to server as an address reference among the door access control and key management systems, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each door access control and key management system and its associated unique key ID codes and unique door ID codes and each door access control and key management system contains the address of the Meta Server."

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or descry bed as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2) Claim 9 is rejected under 35 U.S.C 103(a) as being un-patentable over Martin et al. (U.S 5,979,754) in view of Flick (U.S 6,130,606)

In referring to claim 9, the limitation:

"Wherein the communication and authorization process between the door/key administering system and door control/clock assembly are carried out in a form of encrypted signals or message" is not disclosed by Martin

However, Flick discloses a vehicle security system includes a controller may alternately generates door lock and un-lock commands responsive to the remote transmitter. Flick discloses

the security system simply ignores signals other than properly encrypted signals from the remote transmitter, see (Flick: abstract, lines 1, 14-15; column 1, lines 64-67; column 2, lines 1-7). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "wireless information signals" of Martin to "encrypted signals" that are sent from remote transmitter to receiver which is connected to microprocessor of vehicle security system as taught in York. The combination would have been obvious because on of ordinary skill in the art would have been motivated to deter vehicle theft see (Flick; column 1, lines 24-25).

3) Claim 14 is rejected under 35 U.S.C 103(a) as being un-patentable over Martin et al. (U.S 5,979,754) in view of Dunhame et al. (U.S 5,541,585)

In referring to claim 14, the limitation:

"Wherein the door control/lock assembly further includes means for assisting in the operation of the assembly and sensing the status of the assembly, the means including one or more of the following: a door open sensor, a speaker and microphone assembly, a camera, an activity fight, a buzzer, a call button, a battery condition sensor, a smoke sensor, a temperature sensor" is not disclosed by Martin

However Dunhame discloses a security system for controlling building access that includes door open sensor, speaker and microphone, "dim light" which is equivalent to "activity light" and camera, see (Dunhame: column 5, lines 14-48; column 6, lines 51; column 7, lines 28-29). Dunhame's security system meets the limitation "door control/lock assembly further includes means for assisting in the operation of the assembly and sensing the status of the assembly, the means including one or more of the following: a door open sensor, a speaker and

microphone assembly, a camera, an activity fight." It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "guest room door" of Martin to "controlled portal such as door" which has mechanisms for securing the door such as door open sensor, speaker and microphone, "dim light" which is equivalent to "activity light" and camera as taught by Dunhame. The combination would have been obvious because on of ordinary skill in the art would have been motivated to control access of persons through a controlled door (Dunhame: abstract, lines 1-4).

4) Claims 11-12, 21-22 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin et al. (U.S 5,979,754) in view of Yulkowski (U.S 6,049,287)

In referring to claims 11and 22, the limitation:

4a) "Wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using anyone of the different keys" is not disclosed by Martin

However Yulkowski discloses a door system with electrical components associated therewith for sensing and reacting to emergency conditions. In this invention, Yulkowski discloses a controller may be an access control device has both a "keypad and card reader" those are equivalent to "identification devices". Yulkowski taught that the card reader may be used to insert or slide a card to unlock or lock door, and the key-pad allows the input of an identification code to controller to allow the door to unlock or lock, see (Yulkowski: column 4, lines 59-67). Yulkowski's door system meets the limitation "Wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned

two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using anyone of the different keys." It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin to "door controller" may be an access control device as a key-pad and a card reader, wherein key-pad allows the input of identification code and card reader to insert or slide a card therethrough to unlock or lock the door is taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

In referring to claim 12, the limitation:

4b) "Wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using all or several of the different keys" is not disclosed by Martin

However Yulkowski discloses a controller may be an access control device has both "keypad and card reader" those are equivalent to "identification devices". Yulkowski taught that the card reader and the keypad may intersect so that both a card and an identification code are required to gain access within an opening, see (Yulkowski: column 4, lines 59-67). Yulkowski's door system meets limitation "Wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using all or several of the different keys." It would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin to "door controller" so that both a card identification and an identification code are required to gain access within an opening as taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

In referring to claim 21, the limitation:

4c) "Storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door" is not disclosed by Martin

However Yulkowski discloses a controller may be an access control device has both "keypad and card reader" those are equivalent to "identification devices", that means each identification device must has predetermined key signature for the user. Yulkowski taught that card reader and keypad may intersect so that both a card and an identification code are required to gain access within an opening, see (Yulkowski: column 4, lines 59-67). Yulkowski's door system meets limitation "Storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door." It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "door control unit" of Martin to "door controller" so that both a card identification and an identification code are required to gain access within an opening as taught in Yulkowski. The combination would have been obvious because on of ordinary skill in the art would have been motivated to provide various degrees of security (Yulkowski: column 5, lines 1-4).

5) Claims 6-7, 19, 23, 26, 27 are rejected under 35 U.S.C 103(a) as being un-patentable over Martin et al. (U.S 5,979,754) in view of Kalajan (U.S 6,006,258)

In referring to claims 6, 23, 26, the limitations:

5a) "The door/key administering system includes a door/key administering server system" is matched (Martin: column 3, lines 44-49; column 4, lines 66-67; column 5, lines –32; column 7, lines 30-44)

Martin discloses a control system which may be located at a central control center, this system includes a "computer" is equivalent to "door/key administering server" that stores identity of rooms and doors and "associated credit cards" which is equivalent to "room keys. " Martin's door control system meets the limitation "The door/key administering system includes a door/key administering server system." But Martin does not disclose the communications network includes an Internet Protocol communication.

However Kalajan discloses method of remote access destination network resources through transport protocols, see (Kalajan: column 3, lines 5-27). Kalajan's method meets the limitation "wherein the communications network includes an IP (Internet Protocol) communications network." It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "computer" of Martin to "server" which is remotely access through an Internet protocol by client or employee as taught in Kalajan. The combination would have been obvious because on of ordinary skill in the art would have been motivated to remotely access destination network resources through Internet protocols, see (Kalajan: column 3, lines 5-27).

In referring to claims 7, 19, 27, the limitation:

5b) "Wherein the door control/lock assembly and the door/key administering server system are adapted to be controlled via a web browser operatively connected to the IP communications network" does not disclose by Martin

However, Kalajan discloses an employee can access "server" which is equivalent to "door/key administering server" by using a web browser through IP network, see (Kalajan: column 3, lines 50-67). Kalajan's method meets the limitation "Wherein the door control/lock assembly and the door/key administering server system are adapted to be controlled via a web browser operatively connected to the IP communications network." It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify "computer" of Martin to "server" which is remotely access through an Internet protocol by client or employee as taught in Kalajan. The combination would have been obvious because on of ordinary skill in the art would have been motivated to remotely access destination network resources through Internet protocols, see (Kalajan: column 3, lines 5-27).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to lan dai thi truong whose telephone number is 571-272-7959. The examiner can normally be reached on monday- friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lan Dai Thi Truong
Examiner
Art Unit 2132

Ldt
03/16/2005

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100